# SECURE CRYPTO BIOMETRIC SYSTEM FOR CLOUD COMPUTING

[1] M.*Sudhakar,* [2]*Erra Dharshith,* [3]*Sidda ram sai Santosh mani Teja,* [4]*Kottinti Akshaya ,* [5]*Vakiti Sony*

[1]Assistant Professor in Department of CSE Sreyas Institute of Engineering and Technology

[2.3.4.5]UG Scholar in Department of CSE Sreyas Institute of Engineering and Technology

**Abstract**

Cloud computing has achieved maturity, and there is a heterogeneous group of providers and cloud-based services. However, significant attention remains focused on security concerns. In many cases, security and privacy issues are a significant barrier to user acceptance of cloud computing systems and the advantages these offer with respect to previous systems. Biometric technologies are becoming the key aspect of a wide range of secure identification and personal verification solutions, but in a cloud computing environment they present some problems related to the management of biometric data, due to privacy regulations and the need to trust cloud providers. To overcome those problems in this paper, we propose a crypto biometric system applied to cloud computing in which no private biometric data are exposed.

**Keywords:** *Cloud Computing*

## I INTRODUCTION

Cloud computing is a trend in application architecture and development, as well as a new business model. The success of many service providers, with Amazon as a remarkable example, has demonstrated that the model can be applied to a wide variety of solutions, covering the different levels defined in the cloud paradigm (SaaS, PaaS and IaaS). We can consider that cloud computing is at a mature stage, although there remain some limitations and challenges. Cloud computing brings important benefits for organizations that outsource data, applications, and infrastructure, at the cost of delegating data control. The information is processed in computers that the users do not own, operate, or manage. In this scenario, the user does not know how the provider handles the information, and therefore a high level of trust is needed. The lack of control

over physical and logical aspects of the system imposes profoundchanges in security and privacy procedures. Currently there is even a lack of service level agreements between providers and users regarding security. Our research focuses on adequate security mechanisms that should potentially meet the legal requirements of traditional systems. In recent years, intense research work has been devoted to biometrics, and their applications to security have become more evident. The combination of cloud computing and biometric technology opens new research and implementation opportunities to protect user data in the cloud. However, biometric templates must remain secure even for cloud services providers given the privacy-sensitive nature of biometric data. This requisite is more important than in the case of alphanumerical passwords due to the impossibility of changing user information in the same way.

Instead of storing files on a storage device or hard drive, a user can save them on cloud, making it possibleto access the files from anywhere, as long as they have access to the web. The services hosted on cloud can be broadly divided into infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). Based on the deployment model, cloud can also be classified as public, private, and hybrid cloud.

Further, cloud can be divided into two different layers, namely, front-end and back-end. The layer with which users interact is called the front-end layer. This layer enables a user to access the data that has been stored in cloud through cloud computing software. The layer made up of software and hardware, i.e., thecomputers, servers, central servers, and databases, is the back-end layer. This layer is the primary component of cloud and is entirely responsible for storing information securely. To ensure seamless

connectivity between devices linked via cloud computing, the central servers use a software called middleware Opens a new window that acts as a bridge between the database and applications.

## II LITERATURE SURVEY

***Secure crypto-biometric system for cloud computing, David González Martínez; Francisco Javier González Castaño; Enrique Argones Rúa;***

José Luis Alba Castro; Cloud computing has achieved maturity, and there is a heterogeneous group of

providers and cloud-based services. However, significantattention remains focused on security concerns. In many cases, security and privacy issues are a significant barrier to user acceptance of cloud computing systems and the advantages these offer with respect to previous systems. Biometric technologies are becoming the key aspect of a wide range of secure identification and personal verification solutions, but in a cloud computing environment they present some problems related to the management of biometric data, due to privacy regulations and the need to trust cloud providers. To overcome those problems in this paper, we propose a cryptobiometric system applied to cloud computing in which no private biometric data are exposed..

***Cognitive and Biometric Approaches to Secure Services Management in Cloud-Based Technologies, Marek Ogiela;***

Lidia Ogiela, This article describes new ideas for applying security procedures to data and service management in cloud and fog computing. Management in cloud computing is presented in connection with cognitive systems supporting management tasks and securingimportant data. The application of cognitive and biometric features allows creation of personalized procedures oriented at particular users or a group of protocol participants.

## III EXISTING SYSTEM

The data are stored in the user infrastructure, information location and protection mechanisms are knownin detail. In contrast, a characteristic of public cloud computing services is that the user is completely unaware of data location. This makes it impossible to ensure that national compulsory regulations are met. For example, European data protection laws may impose extra constraints on the handling and processing of data that are transferred to the USA, so the use of Amazon S3 resources to store biometric templates could infringe the law. Several techniques have been proposed for biometric template protection. Among them, cancelable biometrics [10] is one of the most promising. It satisfies a double goal: i) unrecoverability of the original biometric data from the stored biometric template (non- invertibility), and ii) the issue of a new biometric template when an existing template is compromised (renewability).

**Disadvantages**

- Less security compare to proposed system. Centralised applications might cause security issues.

- May be loss of data occurs.

## IV PROPOSED SYSTEM

The purpose of the project is to develop a secure crypto-biometric system for cloud computing. Cloud computing has become increasingly popular, enabling users to store and access their data remotely. However, security concerns have also risen due to the sensitive nature of the data being stored and transmitted. This project aims to address these concerns by combining the power of cryptography and biometric authentication. The system will employ advanced cryptographic algorithms to ensure the confidentiality, integrity, and authenticity of the data stored in the cloud. These algorithms will encrypt the data before transmission and decrypt it upon retrieval, protecting it from unauthorized access or tampering. Additionally, the system will utilize biometric authentication techniques, such as fingerprint or iris scanning, to verify the identity of users accessing the cloud resources. By integrating cryptography and biometrics, the system will provide robust and multi-layered security framework. It will prevent unauthorized access to the cloud infrastructure and ensure that only authenticated individuals with verified biometric credentials can interact with the data stored in the cloud. This approach eliminates the risks associated with traditional password-based authentication systems, such as password cracking or sharing. Overall, the secure crypto-biometric system for cloud computing aims to enhance data security, privacy, and access control in the cloud environment. It provides a reliable and efficient solution for individuals and organizations seeking to protect their sensitive information while leveraging the benefitsof cloud computing.

### *Advantages*

Advantages of the project is to develop a secure crypto-biometric system specifically designed for cloudcomputing environments. The objective is to enhance the overall security of cloud-based applications by combining cryptographic techniques with biometric authentication. The system will employ state-of-the-art encryption algorithms to protect the confidentiality and integrity of data stored in the cloud. Additionally, it will leverage biometric authentication methods, such as fingerprint or iris recognition, toensure

secure access to the cloud resources. By integrating these two powerful security measures, the project aims to provide a robust and multi-layered defense against unauthorized access and data breaches. The system will be designed to seamlessly integrate with existing cloud platforms, allowing users to securely store and access their data without compromising usability. It will also incorporate mechanisms for secure key management, ensuring that cryptographic keys used for data encryption are properly stored and protected. The project will involve developing and implementing novel cryptographic protocols and biometric authentication algorithms. Extensive testing and evaluation will be conducted to ensure the system's effectiveness and resilience against various attack vectors. Furthermore, the project will consider scalability and performance aspects to ensure that the proposed solution can handle large-scale cloud deployments. The final deliverable will be a comprehensive and secure cryptobiometric system that can be readily integrated into cloud computing environments, providing enhanced security for sensitive data stored and processed in the cloud

## V IMPLEMENTATION

1) Upload Fish Dataset:

   using this module we will upload dataset to application

2) Run Interpolation, CLAHE & LAB:

   using this module we will read all images and then apply interpolation, CLAHE and LAB to process allimages and then normalize images and then split dataset into train and test

3) Run Decision Tree:

   processed train images will be input to decision tree to trained a model and this model will be appliedon TEST images to calculate prediction accuracy and other metrics

4) Run Logistic Regression:

   processed train images will be input to logistic regression to trained a model and this model will beapplied on TEST images to calculate prediction accuracy and other metrics

5) Run Naive Bayes:

   processed train images will be input to naïve bayes to trained a model and this model will be applied onTEST images to calculate prediction accuracy and other metrics

6) Run Propose SVM Algorithm:

   processed train images will be input to SVM algorithm to trained a model and this model will be appliedon TEST images to calculate prediction accuracy and other metrics

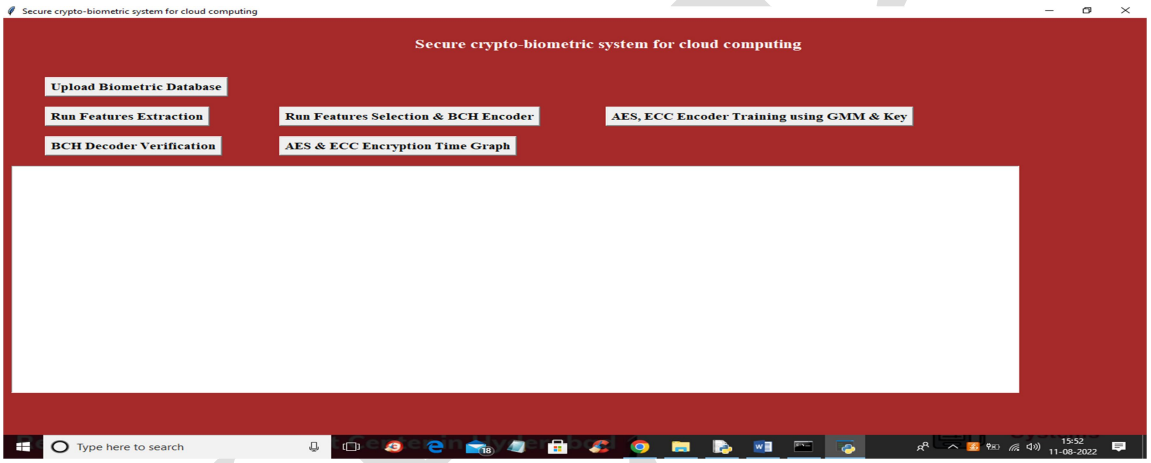
7) Comparison Graph:

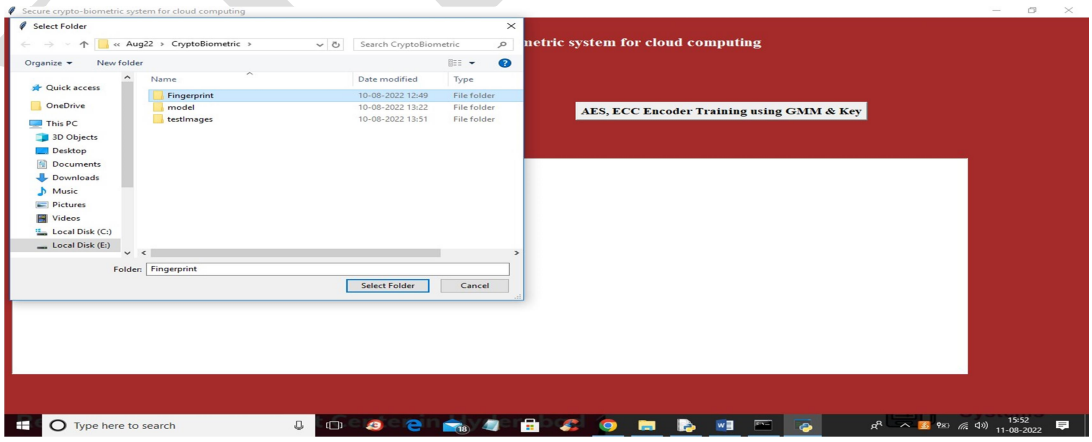
using this module we will plot accuracy and other metric graphs

8) Predict Fish Status:

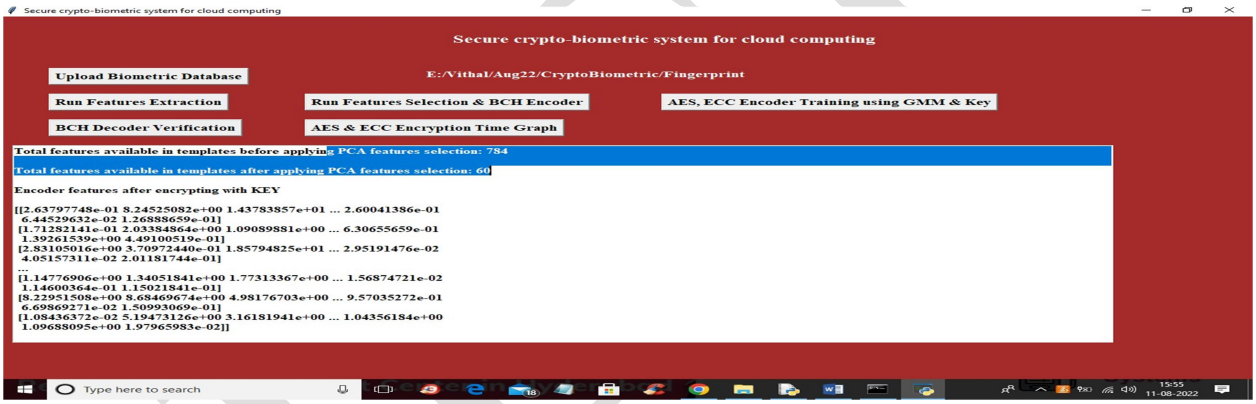
using this module we will upload test image and then SVM algorithm will predict whether imagecontains fresh or infected fish.

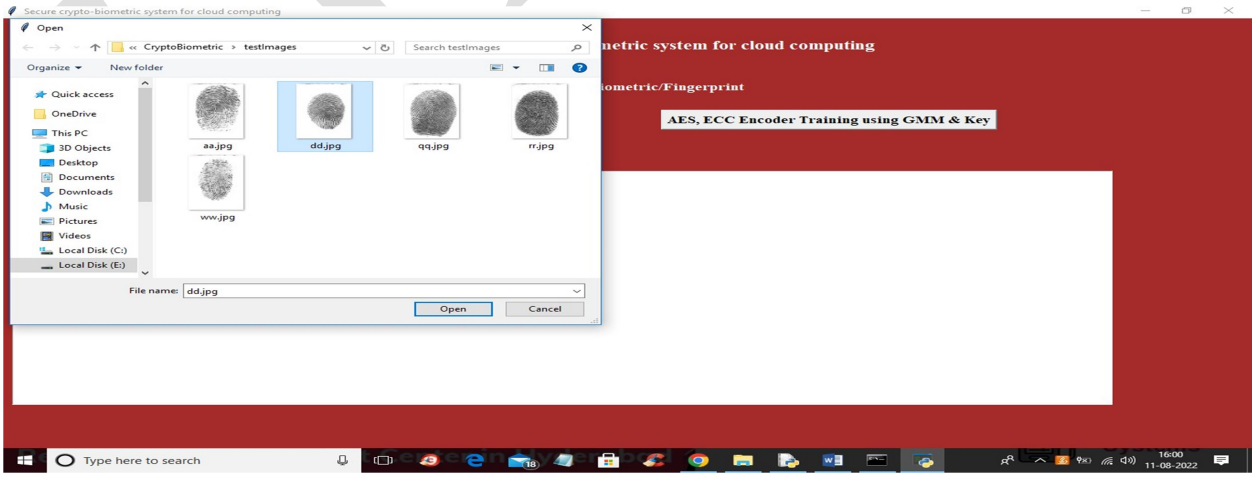
## VI RESULTS

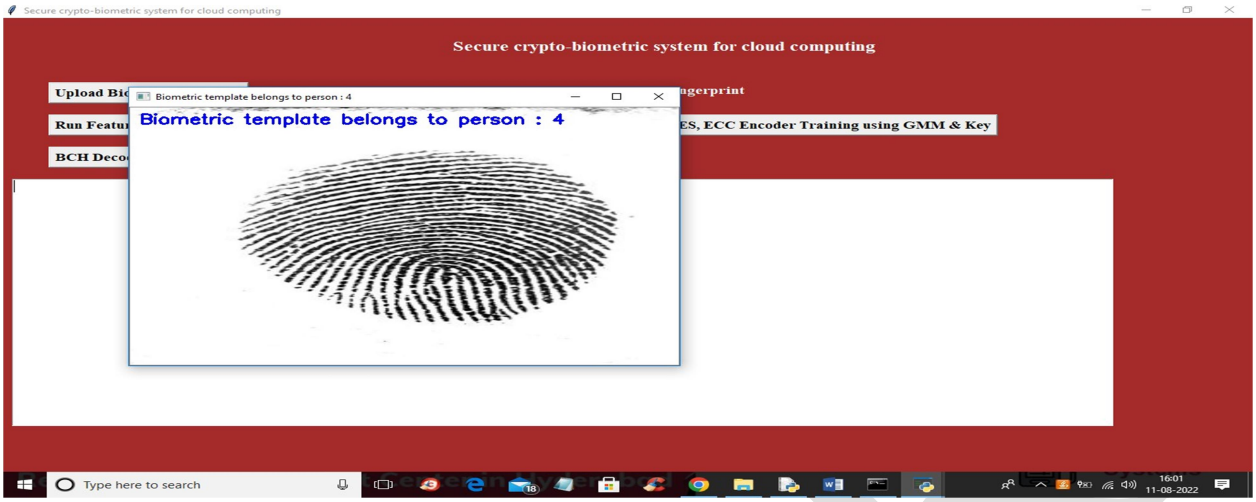


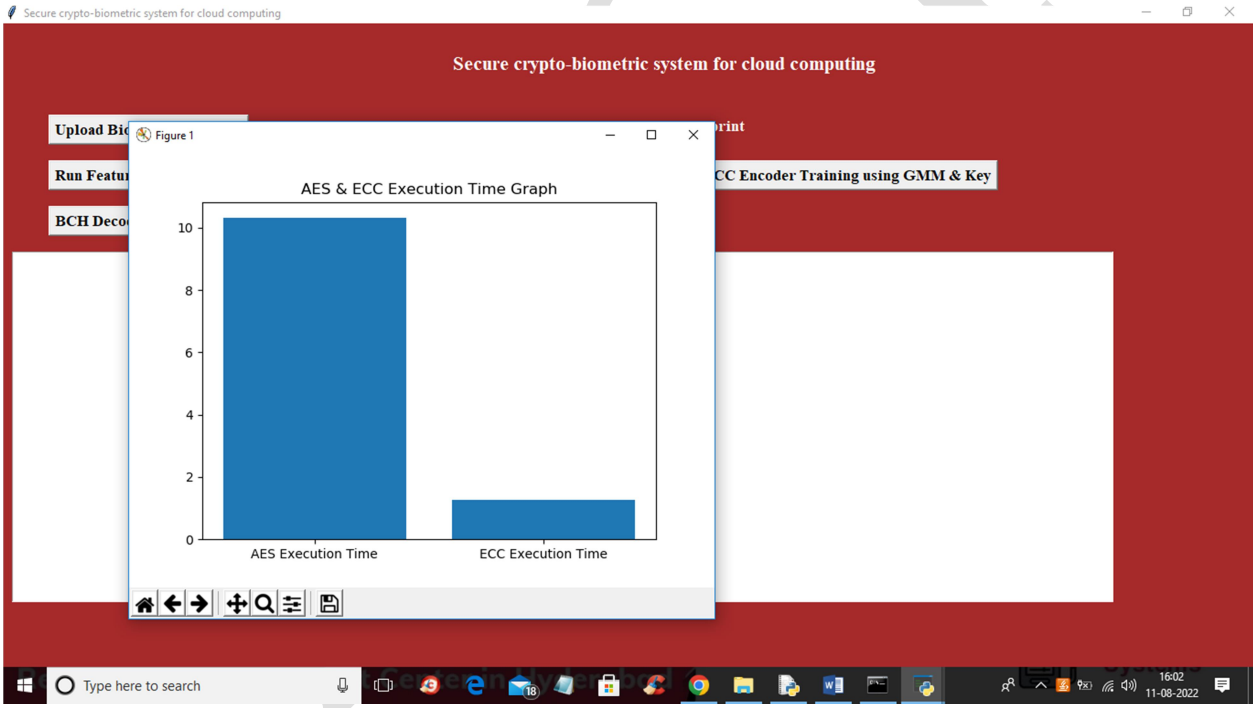




Secure crypto-biometric system for cloud computing
Secure crypto-biometric system for cloud computing
Upload Biometric Database
E:/Vithal/Aug22/CryptoBiometric/Fingerprint
Run Features Extraction
Run Features Selection & BCH Encoder
AES, ECC Encoder Training using GMM & Key
BCH Decoder Verification
AES & ECC Encryption Time Graph
Extracted Features from templates
[[0.99607843 0.85490197 0.5058824 ... 1. 1. 1. ]
[1. 0.85882354 0.4 ... 0.99607843 1. 1. ]
[0.99607843 0.93333334 0.5803922 ... 1. 1. 1. ]
...
[0.98039216 0.8980392 0.5058824 ... 1. 1. 1. ]
[0.99215686 0.8980392 0.5137255 ... 1. 1. 1. ]
[1. 0.9529412 0.5686275 ... 0.99607843 1. 1. ]]
Type here to search
15:54
11-08-2022


Secure crypto-biometric system for cloud computing
Secure crypto-biometric system for cloud computing
Upload Biometric Database
E:/Vithal/Aug22/CryptoBiometric/Fingerprint
Run Features Extraction
Run Features Selection & BCH Encoder
AES, ECC Encoder Training using GMM & Key
BCH Decoder Verification
AES & ECC Encryption Time Graph
Total features available in templates before applying PCA features selection: 784
Total features available in templates after applying PCA features selection: 60
Encoder features after encrypting with KEY
[[2.63797748e-01 8.24525082e+00 1.43783857e+01 ... 2.60041386e-01
6.44529632e-02 1.26888659e-01]
[1.71282141e-01 2.03384864e+00 1.09089881e+00 ... 6.30655659e-01
1.39261539e+00 4.49100519e-01]
[2.83105016e+00 3.70972440e-01 1.85794825e+01 ... 2.95191476e-02
4.05157311e-02 2.01181744e-01]
...
[1.14776906e+00 1.34051841e+00 1.77313367e+00 ... 1.56874721e-02
1.14600364e-01 1.15021841e-01]
[8.22951508e+00 8.68469674e+00 4.98176703e+00 ... 9.57035272e-01
6.69869271e-02 1.50993069e-01]
[1.08436372e-02 5.19473126e+00 3.16181941e+00 ... 1.04356184e+00
1.09688095e+00 1.97965983e-02]]
Type here to search
15:55
11-08-2022


Secure crypto-biometric system for cloud computing
Open
CryptoBiometric › testImages
Search testImages
Organize
New folder
Quick access
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Local Disk (E:)
aa.jpg
dd.jpg
qq.jpg
rr.jpg
ww.jpg
File name: dd.jpg
Open
Cancel
AES, ECC Encoder Training using GMM & Key
Type here to search
16:00
11-08-2022




## VII CONCLUSION

We introduce a significant machine learning-based classification model (SVM) to identify infected fishes in this research work. The real-world without augmented dataset (163 infected and

68 fresh) andaugmented dataset (785 infected and 320 fresh) are used to train our model is new and novel. We mainlyclassify fishes into two individual classes: fresh fish and another is infected fish. We appraise our model with various metrics and show the classified outcome with visual interaction from those classification results. Besides developing our classifier, we applied updated image process ing techniques like k-means segmentation, cubic spline interpolation, and adaptive histogram equalization for transforming our inputimage more adaptable to our classifier. We also compare our model results with three classification models and observe that our proposed classifier is the best solution in this case. This work contributes to bringing out a superior automated fish detection system than the existed systems based on image processing or lower accuracy. We not only depend on the modern image processing technique but also adjoin demandable supervised learning techniques. We prosperously develop the classifier that predicts infected fish with the best accuracy rate than other systems for our real-world novel dataset.

## REFERENCES

[1] A. A. M. Abd Hamid, N. and A. Izani. Extended cubic b-spline interpolation method applied to linear two-point boundary value problem. World Academy of Science, 62, 2010.

[2] T. Acharya. Median computation-based integrated color interpolation and color space conversion methodology from 8-bit bayer pattern rgb color space to 24-bit cie xyz color space, 2002. US Patent 6,366,692.

[3] A. F. Agarap. An architecture combining convolutional neural network (cnn) and support vector machine (svm) for image classification. arXiv preprint arXiv:1712.03541, 2017.

[4] A. Ben-Hur and J. Weston. A user's guide to support vector machines. In Data mining techniques forthe life sciences, pages 223– 239. Springer, 2010.

[5] S. Bianco, F. Gasparini, A. Russo, and R. Schettini. A new method for rgb to xyz transformation based on pattern search optimization. IEEE Transactions on Consumer Electronics, 53(3):1020–1028, 2007.

[6] E. Bisong. Google colaboratory. In Building Machine Learning and Deep Learning Models on Google Cloud Platform, pages 59–64. Springer, 2019.

[7] A. P. Bradley. The use of the area under the roc curve in the evaluation of machine learning algorithms. Pattern recognition, 30(7):1145– 1159, 1997.

[8] S. A. Burney and H. Tariq. K-means cluster analysis for image segmentation. International Journalof Computer Applications, 96(4), 2014.

[9] M. A. Chandra and S. Bedi. Survey on svm and their application in image classification. InternationalJournal of Information Technology, pages 1–11, 2018.

[10] L. de Oliveira Martins, G. B. Junior, A. C. Silva, A. C. de Paiva, and M. Gattass. Detection of masses in digital mammograms using kmeans and support vector machine. ELCVIA Electronic Letters on Computer Vision and Image Analysis, 8(2):39–50, 2009.

IJESR